US009270705B1

(12) **United States Patent**
Chen et al.

(10) **Patent No.: US 9,270,705 B1**
(45) **Date of Patent: *Feb. 23, 2016**

(54) **APPLYING SECURITY POLICY TO AN APPLICATION SESSION**

(71) Applicant: **A10 Networks, Inc.**, San Jose, CA (US)

(72) Inventors: **Lee Chen**, Saratoga, CA (US); **Dennis Oshiba**, Fremont, CA (US); **John Chiong**, San Jose, CA (US)

(73) Assignee: **A10 Networks, Inc.**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 2 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/323,884**

(22) Filed: **Jul. 3, 2014**

Related U.S. Application Data

(63) Continuation of application No. 14/061,720, filed on Oct. 23, 2013, now Pat. No. 8,813,180, which is a continuation of application No. 13/650,179, filed on Oct. 12, 2012, now Pat. No. 8,595,791, which is a

(Continued)

(51) **Int. Cl.**

H04L 29/06	(2006.01)
G06F 21/00	(2013.01)

(Continued)

(52) **U.S. Cl.**
CPC ***H04L 63/20*** (2013.01); *G06F 21/00* (2013.01); *H04L 51/04* (2013.01); *H04L 63/02* (2013.01);

(Continued)

(58) **Field of Classification Search**
CPC ... H04L 63/20; H04L 63/0227; H04L 67/306; H04L 67/10; H04L 63/02; H04L 65/1026; H04L 63/0407; H04L 51/04; H04M 1/72547; G06F 21/00

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,774,660	A	6/1998	Brendel et al.
5,935,207	A	8/1999	Logue et al.

(Continued)

FOREIGN PATENT DOCUMENTS

CN	1372662	A	10/2002
CN	1449618		10/2003

(Continued)

OTHER PUBLICATIONS

Cardellini et al., "Dynamic Load Balancing on Web-server Systems", IEEE Internet Computing, vol. 3, No. 3, pp. 28-39, May-Jun. 1999.

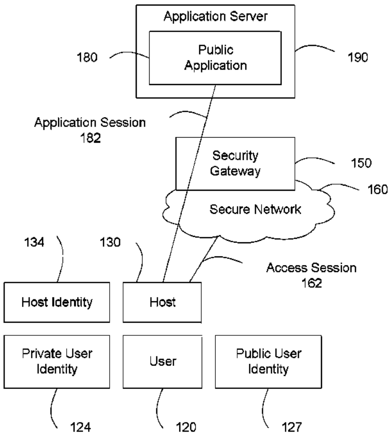
(Continued)

Primary Examiner — Carl Colin
Assistant Examiner — Gary Lavelle
(74) *Attorney, Agent, or Firm* — Carr & Ferrell LLP

(57) **ABSTRACT**

Applying a security policy to an application session, includes: recognizing the application session between a network and an application via a security gateway; determining by the security gateway a user identity of the application session using information about the application session; obtaining by the security gateway the security policy comprising network parameters mapped to the user identity; and applying the security policy to the application session by the security gateway. The user identity may be a network user identity or an application user identity recognized from packets of the application session. The security policy may comprise a network traffic policy mapped and/or a document access policy mapped to the user identity, where the network traffic policy is applied to the application session. The security gateway may further generate a security report concerning the application of the security policy to the application session.

27 Claims, 11 Drawing Sheets



Related U.S. Application Data

continuation of application No. 12/788,339, filed on May 27, 2010, now Pat. No. 8,312,507, which is a continuation-in-part of application No. 12/771,491, filed on Apr. 30, 2010, now Pat. No. 7,979,585, which is a continuation of application No. 11/582,613, filed on Oct. 17, 2006, now Pat. No. 7,716,378.

(51) **Int. Cl.**
H04L 29/08 (2006.01)
H04L 12/58 (2006.01)

(52) **U.S. Cl.**
CPC *H04L 63/0227* (2013.01); *H04L 63/0407* (2013.01); *H04L 65/1026* (2013.01); *H04L 67/10* (2013.01); *H04L 67/306* (2013.01); *H04L 67/42* (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,958,053	A	9/1999	Denker	
6,003,069	A	12/1999	Cavill	
6,047,268	A	4/2000	Bartoli et al.	
6,219,706	B1	4/2001	Fan et al.	
6,321,338	B1	11/2001	Porras et al.	
6,374,300	B2	4/2002	Masters	
6,587,866	B1	7/2003	Modi et al.	
6,748,414	B1	6/2004	Bournas	
6,772,334	B1	8/2004	Glawitsch	
6,779,033	B1	8/2004	Watson et al.	
7,010,605	B1	3/2006	Dharmarajan	
7,058,718	B2	6/2006	Fontes et al.	
7,069,438	B2	6/2006	Balabine et al.	
7,076,555	B1	7/2006	Orman et al.	
7,143,087	B2	11/2006	Fairweather	
7,181,524	B1	2/2007	Lele	
7,228,359	B1	6/2007	Monteiro	
7,234,161	B1	6/2007	Maufer et al.	
7,236,457	B2	6/2007	Joe	
7,254,133	B2	8/2007	Govindarajan et al.	
7,269,850	B2	9/2007	Govindarajan et al.	
7,277,963	B2	10/2007	Dolson et al.	
7,301,899	B2	11/2007	Goldstone	
7,308,499	B2	12/2007	Chavez	
7,310,686	B2	12/2007	Uysal	
7,328,267	B1	2/2008	Bashyam et al.	
7,334,232	B2	2/2008	Jacobs et al.	
7,337,241	B2	2/2008	Boucher et al.	
7,343,399	B2	3/2008	Hayball et al.	
7,349,970	B2	3/2008	Clement et al.	
7,370,353	B2	5/2008	Yang	
7,391,725	B2	6/2008	Huitema et al.	
7,398,317	B2	7/2008	Chen et al.	
7,423,977	B1	9/2008	Joshi	
7,430,755	B1	9/2008	Hughes et al.	
7,467,202	B2	12/2008	Savchuk	
7,472,190	B2	12/2008	Robinson	
7,506,360	B1	3/2009	Wilkinson et al.	
7,512,980	B2	3/2009	Copeland et al.	
7,533,409	B2	5/2009	Keane et al.	
7,552,323	B2	6/2009	Shay	
7,584,262	B1	9/2009	Wang et al.	
7,590,736	B2	9/2009	Hydrie et al.	
7,613,193	B2	11/2009	Swami et al.	
7,613,822	B2	11/2009	Joy et al.	
7,673,072	B2	3/2010	Boucher et al.	
7,675,854	B2	3/2010	Chen et al.	
7,707,295	B1	4/2010	Szeto et al.	
7,711,790	B1	5/2010	Barrett et al.	
7,747,748	B2	6/2010	Allen	
7,792,113	B1	9/2010	Foschiano et al.	
7,826,487	B1	11/2010	Mukerji et al.	
7,881,215	B1	2/2011	Daigle et al.	
7,970,934	B1 *	6/2011	Patel	H04L 41/147 709/244
7,990,847	B1	8/2011	Leroy et al.	
7,991,859	B1	8/2011	Miller et al.	
8,090,866	B1	1/2012	Bashyam et al.	
8,122,116	B2	2/2012	Matsunaga et al.	
8,185,651	B2	5/2012	Moran et al.	
8,191,106	B2 *	5/2012	Choyi	H04L 63/20 713/150
8,224,971	B1	7/2012	Miller et al.	
8,296,434	B1	10/2012	Miller et al.	
8,312,507	B2	11/2012	Chen et al.	
8,379,515	B1	2/2013	Mukerji	
8,554,929	B1	10/2013	Szeto et al.	
8,560,693	B1	10/2013	Wang et al.	
8,584,199	B1	11/2013	Chen et al.	
8,595,791	B1	11/2013	Chen et al.	
RE44,701	E	1/2014	Chen et al.	
8,681,610	B1	3/2014	Mukerji	
8,782,221	B2	7/2014	Han	
8,813,180	B1	8/2014	Chen et al.	
8,826,372	B1	9/2014	Chen et al.	
8,885,463	B1	11/2014	Medved et al.	
8,897,154	B2	11/2014	Jalan et al.	
8,965,957	B2	2/2015	Barros	
8,977,749	B1	3/2015	Han	
8,990,262	B2	3/2015	Chen et al.	
9,094,364	B2	7/2015	Jalan et al.	
9,106,561	B2	8/2015	Jalan et al.	
2001/0049741	A1	12/2001	Skene et al.	
2002/0032777	A1	3/2002	Kawata et al.	
2002/0078164	A1	6/2002	Reinschmidt	
2002/0091844	A1	7/2002	Craft et al.	
2002/0103916	A1	8/2002	Chen et al.	
2002/0133491	A1	9/2002	Sim et al.	
2002/0138618	A1	9/2002	Szabo	
2002/0143991	A1	10/2002	Chow et al.	
2002/0178259	A1	11/2002	Doyle et al.	
2002/0194335	A1	12/2002	Maynard	
2002/0194350	A1	12/2002	Lu et al.	
2003/0009591	A1	1/2003	Hayball et al.	
2003/0014544	A1	1/2003	Pettey	
2003/0023711	A1	1/2003	Parmar et al.	
2003/0023873	A1	1/2003	Ben-Itzhak	
2003/0035409	A1	2/2003	Wang et al.	
2003/0035420	A1	2/2003	Niu	
2003/0131245	A1	7/2003	Linderman	
2003/0135625	A1	7/2003	Fontes et al.	
2003/0195962	A1	10/2003	Kikuchi et al.	
2004/0062246	A1	4/2004	Boucher et al.	
2004/0073703	A1	4/2004	Boucher et al.	
2004/0078419	A1	4/2004	Ferrari et al.	
2004/0078480	A1	4/2004	Boucher et al.	
2004/0111516	A1	6/2004	Cain	
2004/0187032	A1	9/2004	Gels et al.	
2004/0199616	A1	10/2004	Karhu	
2004/0199646	A1	10/2004	Susai et al.	
2004/0202182	A1	10/2004	Lund et al.	
2004/0210663	A1	10/2004	Phillips et al.	
2004/0213158	A1	10/2004	Collett et al.	
2005/0009520	A1 *	1/2005	Herrero	H04L 29/12188 455/435.1
2005/0021848	A1	1/2005	Jorgenson	
2005/0027862	A1	2/2005	Nguyen et al.	
2005/0036501	A1	2/2005	Chung et al.	
2005/0036511	A1	2/2005	Baratakke et al.	
2005/0044270	A1	2/2005	Grove et al.	
2005/0074013	A1	4/2005	Hershey et al.	
2005/0080890	A1	4/2005	Yang et al.	
2005/0102400	A1	5/2005	Nakahara et al.	
2005/0125276	A1 *	6/2005	Rusu	G06Q 30/02 705/304
2005/0163073	A1	7/2005	Heller et al.	
2005/0198335	A1	9/2005	Brown et al.	
2005/0240989	A1	10/2005	Kim et al.	
2005/0249225	A1	11/2005	Singhal	
2006/0023721	A1	2/2006	Miyake et al.	
2006/0036610	A1	2/2006	Wang	
2006/0036733	A1	2/2006	Fujimoto et al.	

(56) References Cited

U.S. PATENT DOCUMENTS

2006/0069774	A1	3/2006	Chen et al.	
2006/0069804	A1	3/2006	Miyake et al.	
2006/0077926	A1 *	4/2006	Rune	H04L 45/34 370/328
2006/0092950	A1	5/2006	Arregoces et al.	
2006/0098645	A1	5/2006	Walkin	
2006/0168319	A1	7/2006	Trossen	
2006/0187901	A1	8/2006	Cortes et al.	
2006/0190997	A1	8/2006	Mahajani et al.	
2006/0251057	A1	11/2006	Kwon et al.	
2006/0277303	A1	12/2006	Hegde et al.	
2006/0280121	A1	12/2006	Matoba	
2007/0019543	A1	1/2007	Wei et al.	
2007/0118881	A1	5/2007	Mitchell et al.	
2007/0156919	A1	7/2007	Potti et al.	
2007/0185998	A1	8/2007	Touitou et al.	
2007/0195792	A1	8/2007	Chen et al.	
2007/0230337	A1	10/2007	Igarashi et al.	
2007/0245090	A1	10/2007	King et al.	
2007/0259673	A1 *	11/2007	Willars	H04W 52/0225 455/453
2007/0283429	A1	12/2007	Chen et al.	
2007/0286077	A1	12/2007	Wu	
2007/0288247	A1	12/2007	Mackay	
2007/0294209	A1 *	12/2007	Strub	H04L 67/22
2008/0031263	A1	2/2008	Ervin et al.	
2008/0101396	A1	5/2008	Miyata	
2008/0109452	A1	5/2008	Patterson	
2008/0109870	A1 *	5/2008	Sherlock	H04L 63/1425 726/1
2008/0134332	A1	6/2008	Keohane et al.	
2008/0228781	A1	9/2008	Chen et al.	
2008/0250099	A1	10/2008	Shen et al.	
2008/0291911	A1	11/2008	Lee et al.	
2009/0049198	A1	2/2009	Blinn et al.	
2009/0070470	A1	3/2009	Bauman et al.	
2009/0077651	A1	3/2009	Poeluev	
2009/0092124	A1	4/2009	Singhal et al.	
2009/0106830	A1	4/2009	Maher	
2009/0138606	A1	5/2009	Moran et al.	
2009/0138945	A1	5/2009	Savchuk	
2009/0141634	A1	6/2009	Rothstein et al.	
2009/0164614	A1	6/2009	Christian et al.	
2009/0172093	A1	7/2009	Matsubara	
2009/0213858	A1	8/2009	Dolganow et al.	
2009/0222583	A1	9/2009	Josefsberg et al.	
2009/0228547	A1	9/2009	Miyaoka et al.	
2010/0008229	A1	1/2010	Bi et al.	
2010/0036952	A1	2/2010	Hazlewood et al.	
2010/0054139	A1	3/2010	Chun et al.	
2010/0061319	A1	3/2010	Aso et al.	
2010/0064008	A1	3/2010	Yan et al.	
2010/0083076	A1	4/2010	Ushiyama	
2010/0094985	A1	4/2010	Abu-Samaha et al.	
2010/0106833	A1	4/2010	Banerjee et al.	
2010/0106854	A1	4/2010	Kim et al.	
2010/0162378	A1	6/2010	Jayawardena et al.	
2010/0210265	A1	8/2010	Borzsei et al.	
2010/0217793	A1	8/2010	Preiss	
2010/0223630	A1	9/2010	Degenkolb et al.	
2010/0228819	A1	9/2010	Wei	
2010/0235507	A1	9/2010	Szeto et al.	
2010/0235522	A1	9/2010	Chen et al.	
2010/0235880	A1	9/2010	Chen et al.	
2010/0265824	A1	10/2010	Chao et al.	
2010/0268814	A1	10/2010	Cross et al.	
2010/0293296	A1	11/2010	Hsu et al.	
2010/0312740	A1	12/2010	Clemm et al.	
2010/0318631	A1	12/2010	Shukla	
2010/0322252	A1	12/2010	Suganthi et al.	
2010/0330971	A1	12/2010	Selitser et al.	
2010/0333101	A1	12/2010	Pope et al.	
2011/0007652	A1	1/2011	Bai	
2011/0023071	A1	1/2011	Li et al.	
2011/0029599	A1	2/2011	Pulleyn et al.	
2011/0032941	A1	2/2011	Quach et al.	
2011/0040826	A1	2/2011	Chadzelek et al.	
2011/0047294	A1	2/2011	Singh et al.	
2011/0060831	A1	3/2011	Ishii et al.	
2011/0093522	A1	4/2011	Chen et al.	
2011/0110294	A1	5/2011	Valluri et al.	
2011/0145324	A1	6/2011	Reinart et al.	
2011/0153834	A1	6/2011	Bharrat	
2011/0185073	A1	7/2011	Jagadeeswaran et al.	
2011/0191773	A1	8/2011	Pavel et al.	
2011/0196971	A1	8/2011	Reguraman et al.	
2011/0276695	A1	11/2011	Maldaner	
2011/0276982	A1	11/2011	Nakayama et al.	
2011/0289496	A1	11/2011	Steer	
2011/0302256	A1	12/2011	Sureshehandra et al.	
2011/0307541	A1	12/2011	Walsh et al.	
2012/0023231	A1	1/2012	Ueno	
2012/0030341	A1	2/2012	Jensen et al.	
2012/0066371	A1	3/2012	Patel et al.	
2012/0084419	A1	4/2012	Kannan et al.	
2012/0084460	A1	4/2012	McGinnity et al.	
2012/0144014	A1	6/2012	Natham et al.	
2012/0144015	A1	6/2012	Jalan et al.	
2012/0170548	A1	7/2012	Rajagopalan et al.	
2012/0173759	A1	7/2012	Agarwal et al.	
2012/0191839	A1	7/2012	Maynard	
2012/0240185	A1	9/2012	Kapoor et al.	
2012/0290727	A1	11/2012	Tivig	
2012/0297046	A1	11/2012	Raja et al.	
2013/0046876	A1	2/2013	Narayana et al.	
2013/0074177	A1	3/2013	Varadhan et al.	
2013/0083725	A1	4/2013	Mallya et al.	
2013/0100958	A1	4/2013	Jalan et al.	
2013/0136139	A1	5/2013	Zheng et al.	
2013/0166762	A1	6/2013	Jalan et al.	
2013/0173795	A1	7/2013	McPherson	
2013/0176854	A1	7/2013	Chisu et al.	
2013/0191486	A1	7/2013	Someya et al.	
2013/0198385	A1	8/2013	Han et al.	
2014/0012972	A1	1/2014	Han	
2014/0089500	A1	3/2014	Sankar et al.	
2014/0164617	A1	6/2014	Jalan et al.	
2014/0169168	A1	6/2014	Jalan et al.	
2014/0207845	A1	7/2014	Han et al.	
2014/0258536	A1	9/2014	Chiong	
2014/0269728	A1	9/2014	Jalan et al.	
2014/0330982	A1	11/2014	Jalan et al.	
2014/0359052	A1	12/2014	Joachimpillai et al.	
2015/0039671	A1	2/2015	Jalan et al.	
2015/0156223	A1	6/2015	Xu et al.	

FOREIGN PATENT DOCUMENTS

CN	1529460		9/2004
CN	1575582		2/2005
CN	1725702		1/2006
CN	101004740	A	7/2007
CN	101094225		12/2007
CN	101189598		5/2008
CN	101247349	A	8/2008
CN	101261644	A	9/2008
CN	102546590		7/2012
CN	102571742		7/2012
CN	102577252		7/2012
CN	102918801		2/2013
CN	103533018	A	1/2014
CN	103944954		7/2014
CN	104040990		9/2014
CN	104067569		9/2014
CN	104106241		10/2014
CN	104137491		11/2014
CN	104796396	A	7/2015
EP	1209876		5/2002
EP	1770915		4/2007
EP	1885096		2/2008
EP	2577910		4/2013
EP	2622795		8/2013
EP	2647174		10/2013
EP	2760170		7/2014

(56) **References Cited**

FOREIGN PATENT DOCUMENTS

EP	2772026		9/2014
EP	2901308	A2	8/2015
HK	1182560		11/2013
HK	1183569	A	12/2013
HK	1183996	A	1/2014
HK	1189438		6/2014
HK	1198565	A1	5/2015
HK	1198848	A1	6/2015
HK	1199153	A1	6/2015
HK	1199779	A1	7/2015
JP	0997233		4/1997
JP	11338836		10/1999
JP	2000276432	A	10/2000
JP	200151859		2/2001
JP	2006332825	A	12/2006
JP	200840718		2/2008
JP	2013528330		5/2011
JP	2014143686		8/2014
JP	2015507380	A	3/2015
KR	10-0830413		5/2008
WO	01/13228		2/2001
WO	0114990		3/2001
WO	WO0145349		6/2001
WO	03103237		12/2003
WO	WO2004084085	A1	9/2004
WO	2008053954		5/2008
WO	2011049770		4/2011
WO	2011149796		12/2011
WO	2012050747		4/2012
WO	2012075237		6/2012
WO	2013070391		5/2013
WO	2013081952		6/2013
WO	2013096019		6/2013
WO	2013112492		8/2013
WO	2014052099		4/2014
WO	2014088741		6/2014
WO	2014093829		6/2014
WO	WO2014138483		9/2014
WO	WO2014144837		9/2014
WO	WO2014179753		11/2014

OTHER PUBLICATIONS

Hunt et al. NetDispatcher: A TCP Connection Router, IBM Research Report RC 20853 May 19, 1997.

Spatscheck et al., “Optimizing TCP Forwarder Performance”, IEEE/ACM Transactions on Networking, vol. 8, No. 2, Apr. 2000.

Kjaer et al. “Resource allocation and disturbance rejection in web servers using SLAs and virtualized servers”, IEEE Transactions on Network and Service Management, IEEE, US, vol. 6, No. 4, Dec. 1, 2009.

Sharifian et al. “An approximation-based load-balancing algorithm with admission control for cluster web servers with dynamic workloads”, The Journal of Supercomputing, Kluwer Academic Publishers, BO, vol. 53, No. 3, Jul. 3, 2009.

Noguchi, “Realizing the Highest Level “Layer 7” Switch” = Totally Managing Network Resources, Applications, and Users =, Computer & Network LAN, Jan. 1, 2000, vol. 18, No. 1, p. 109-112.

Takahashi, “The Fundamentals of the Windows Network: Understanding the Mystery of the Windows Network from the Basics”, Network Magazine, Jul. 1, 2006, vol. 11, No. 7, p. 32-35.

Ohnuma, “AppSwitch: 7th Layer Switch Provided with Full Setup and Report Tools”, Interop Magazine, Jun. 1, 2000, vol. 10, No. 6, p. 148-150.

* cited by examiner

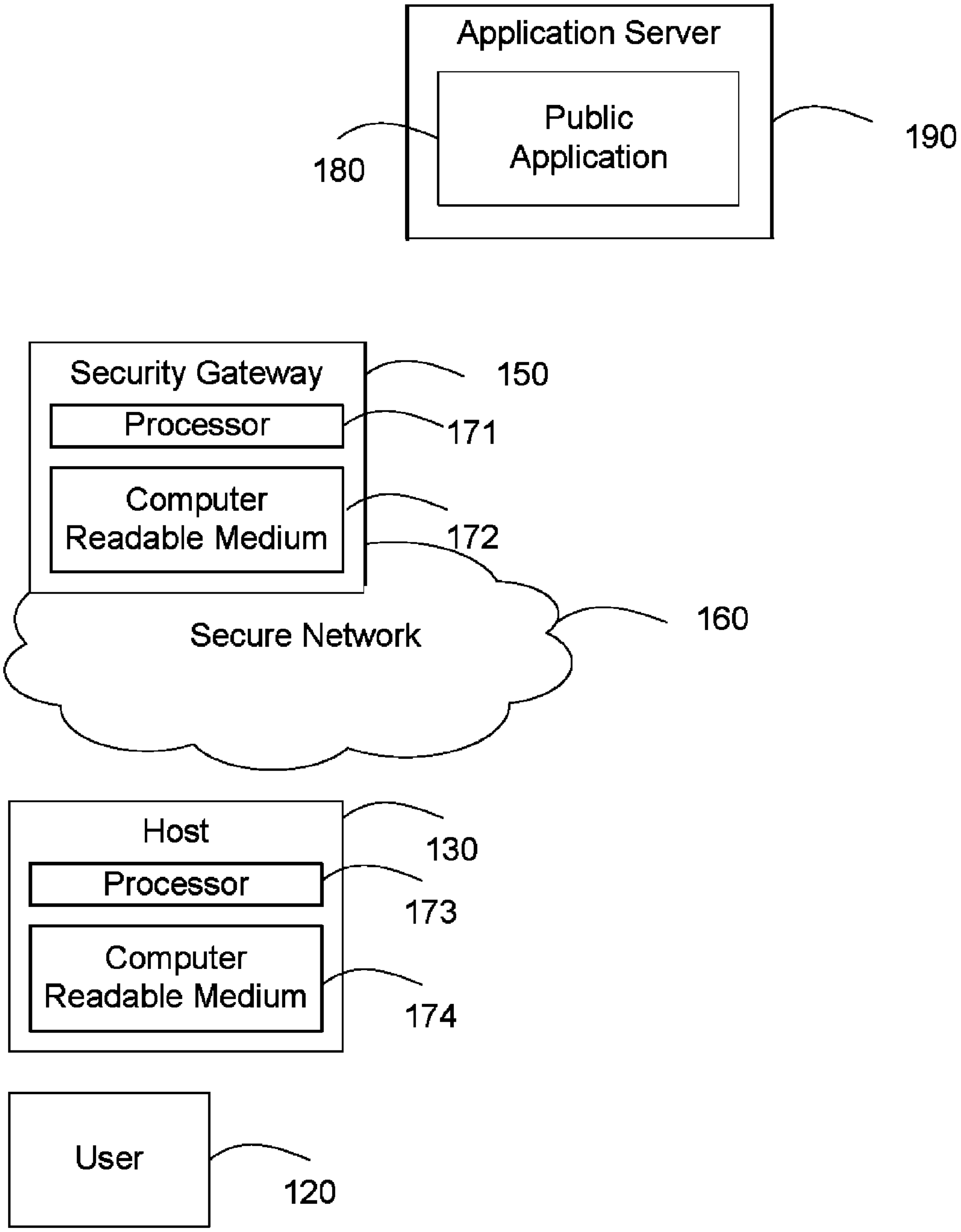

Application Server
Public Application
180
190
Security Gateway
Processor
Computer Readable Medium
150
171
172
Secure Network
160
Host
Processor
Computer Readable Medium
130
173
174
User
120

FIG. 1a

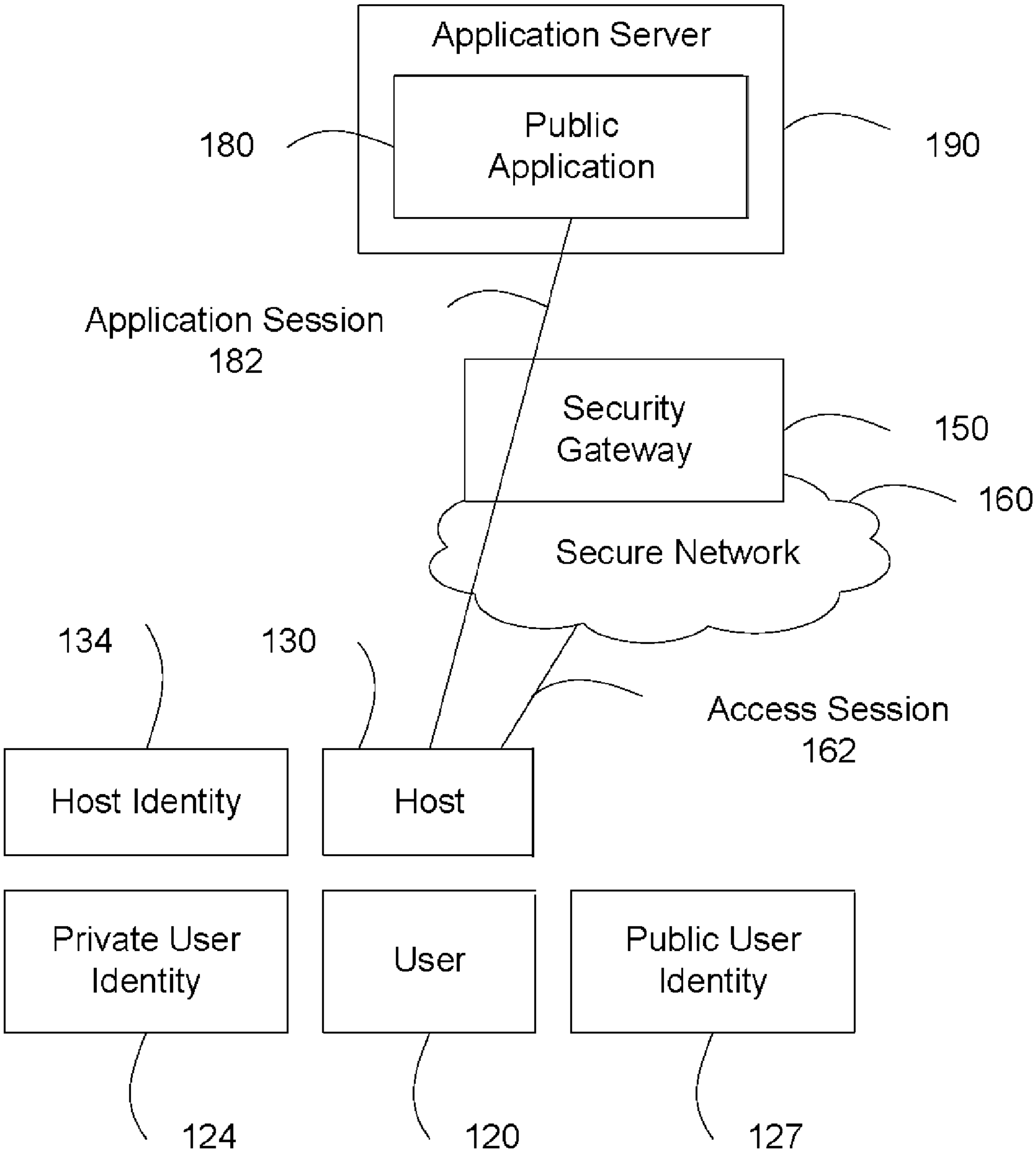

Application Server
Public Application
180
190
Application Session 182
Security Gateway
150
160
Secure Network
134
130
Access Session 162
Host Identity
Host
Private User Identity
User
Public User Identity
124
120
127

FIG. 1b

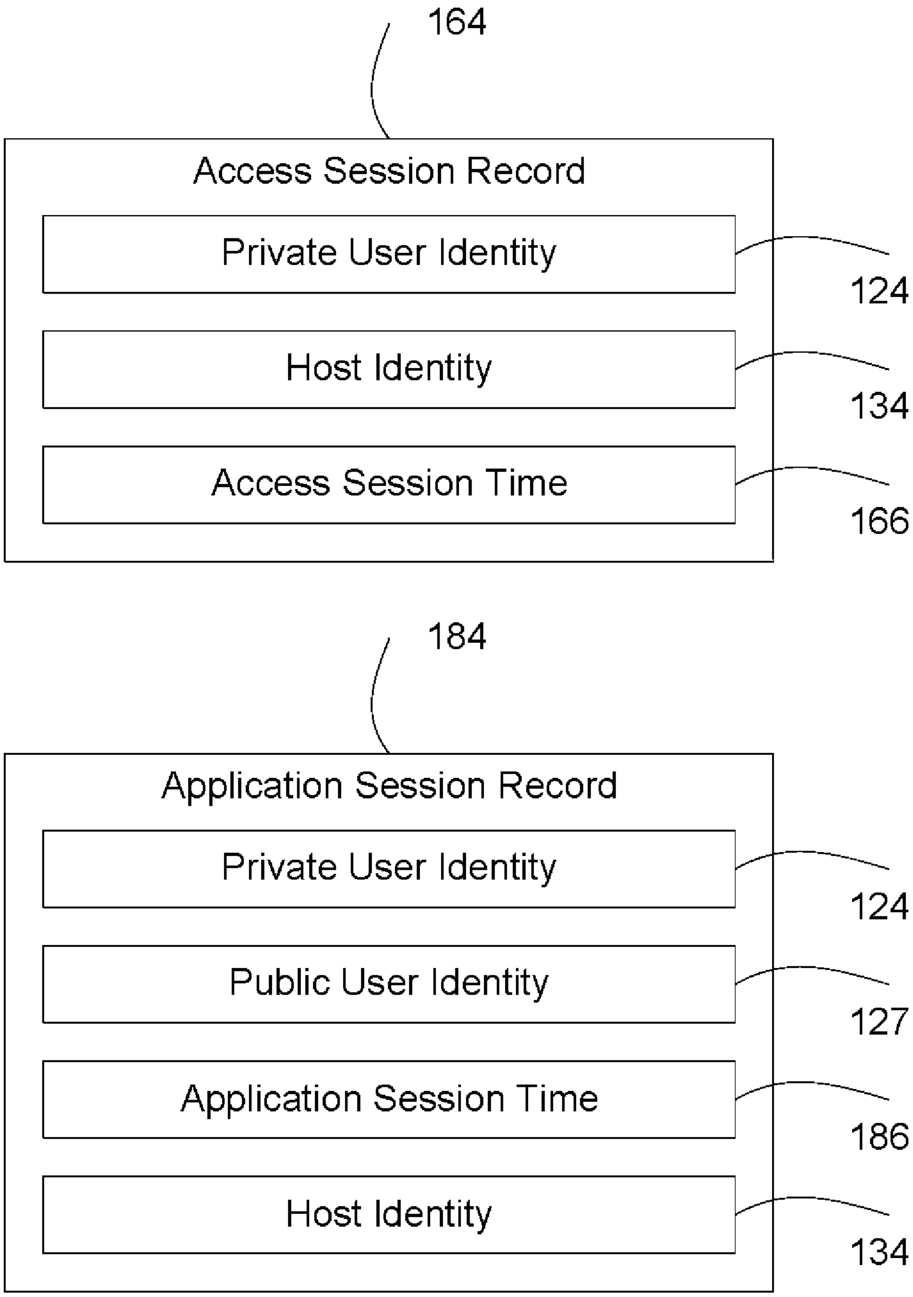

164
Access Session Record
Private User Identity
124
Host Identity
134
Access Session Time
166
184
Application Session Record
Private User Identity
124
Public User Identity
127
Application Session Time
186
Host Identity
134

FIG. 1c

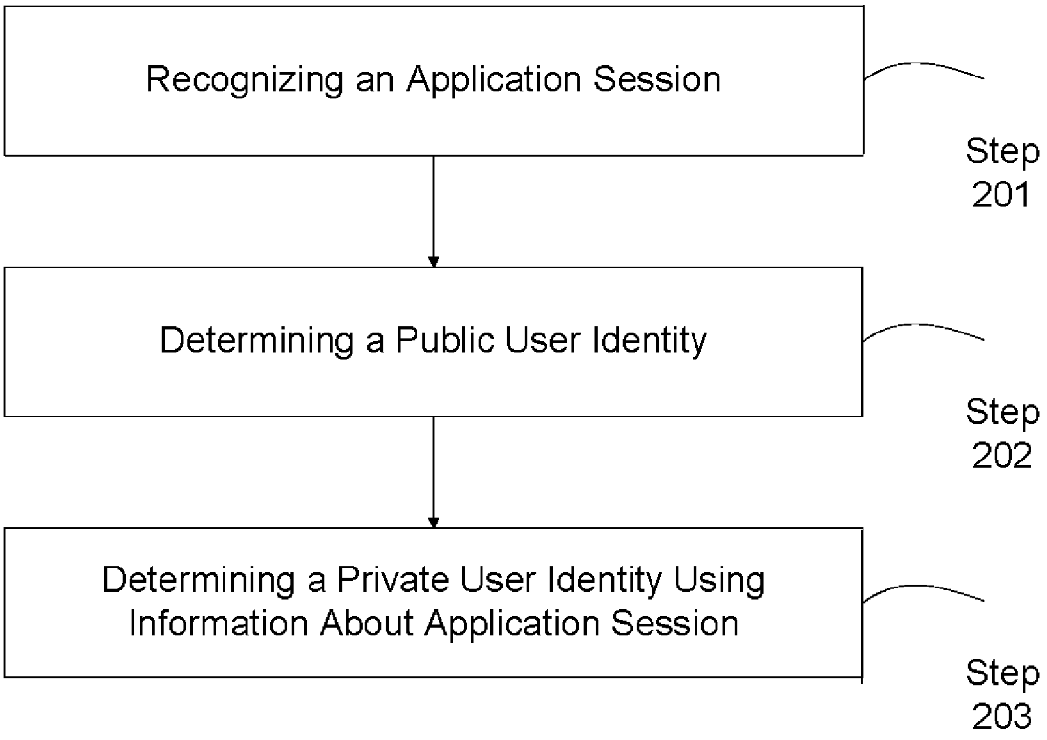

Recognizing an Application Session
Step 201
Determining a Public User Identity
Step 202
Determining a Private User Identity Using Information About Application Session
Step 203

FIG. 2

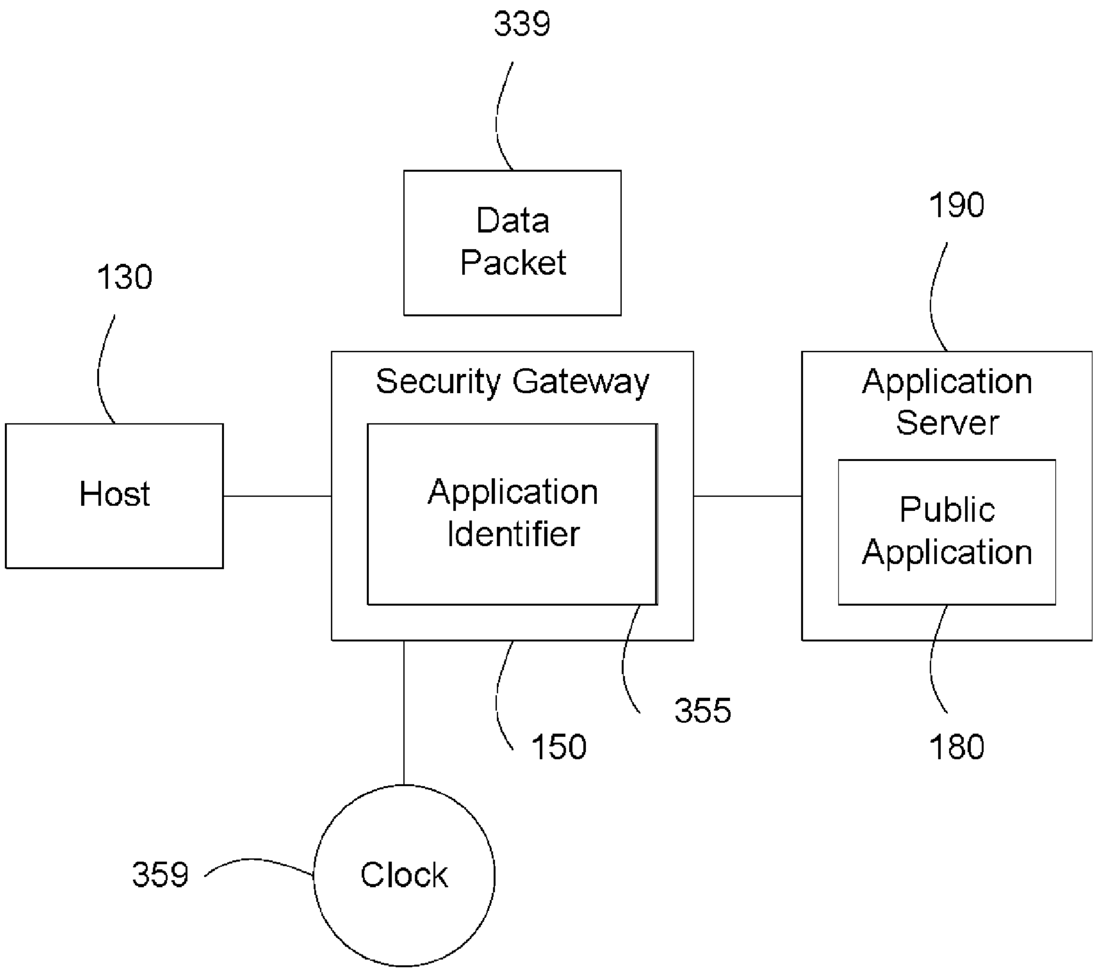

339
Data Packet
190
130
Security Gateway
Application Server
Host
Application Identifier
Public Application
355
150
180
359
Clock

FIG. 3

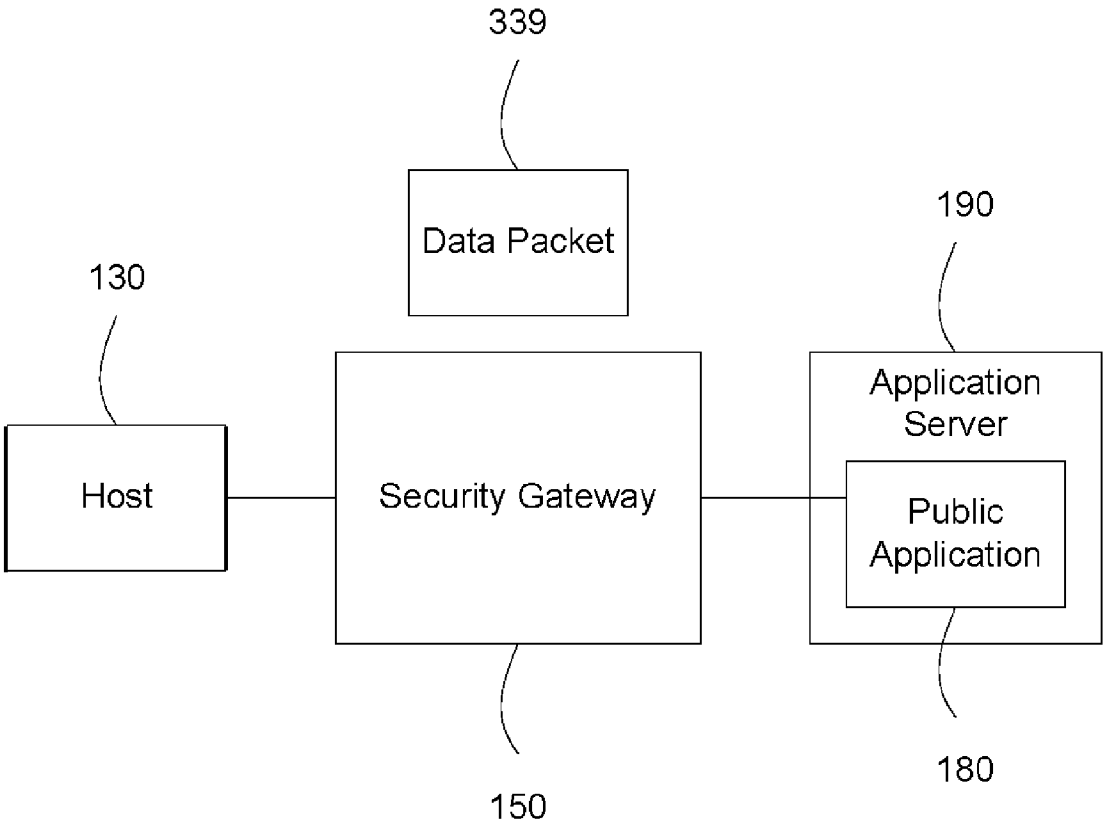

339
Data Packet
190
130
Application Server
Host
Security Gateway
Public Application
150
180

FIG. 4a

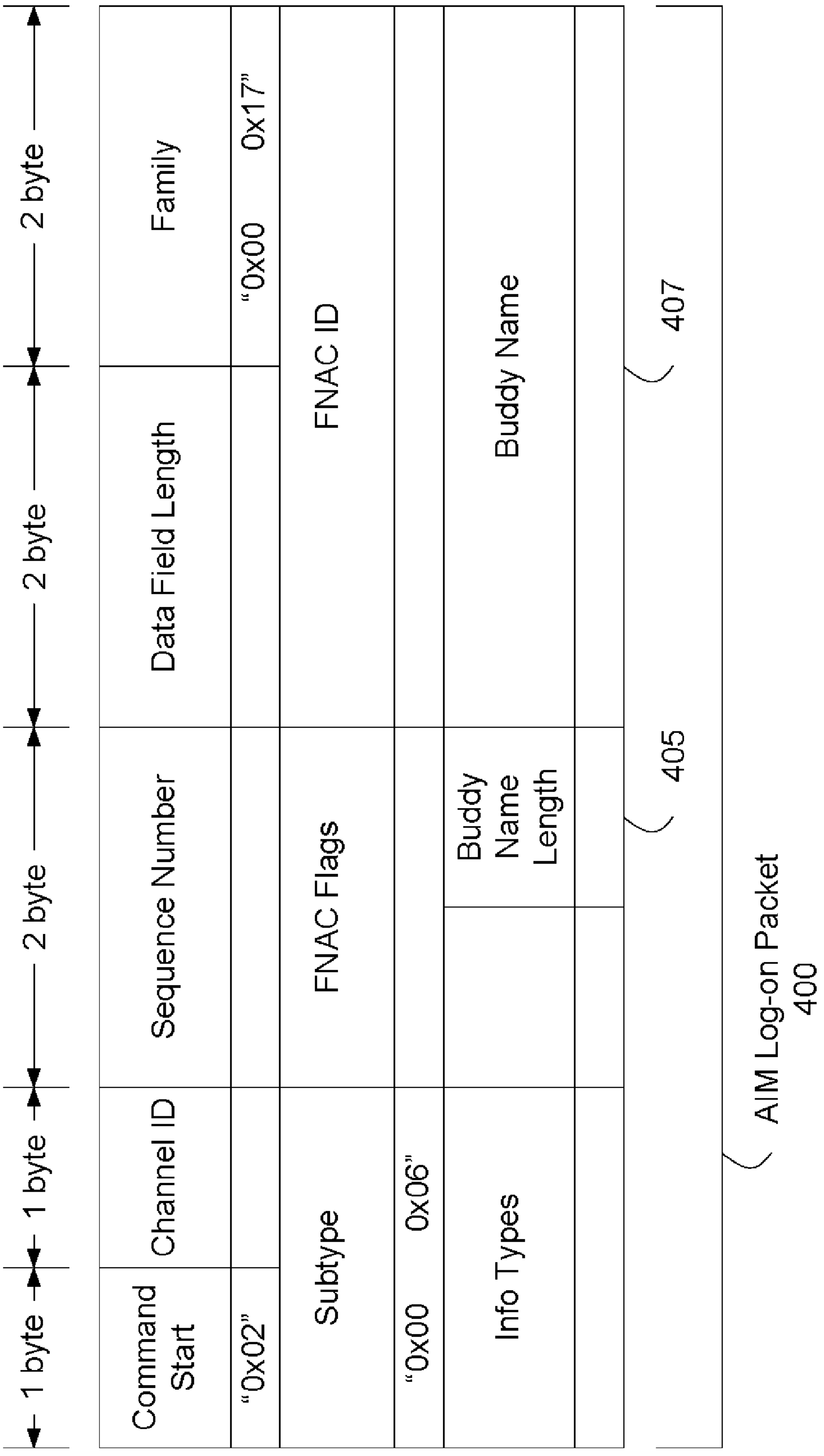

1 byte
1 byte
2 byte
2 byte
2 byte
Command Start
Channel ID
Sequence Number
Data Field Length
Family
"0x02"
"0x00 0x17"
Subtype
FNAC Flags
FNAC ID
"0x00 0x06"
Info Types
Buddy Name Length
Buddy Name
405
407
AIM Log-on Packet 400

FIG. 4b

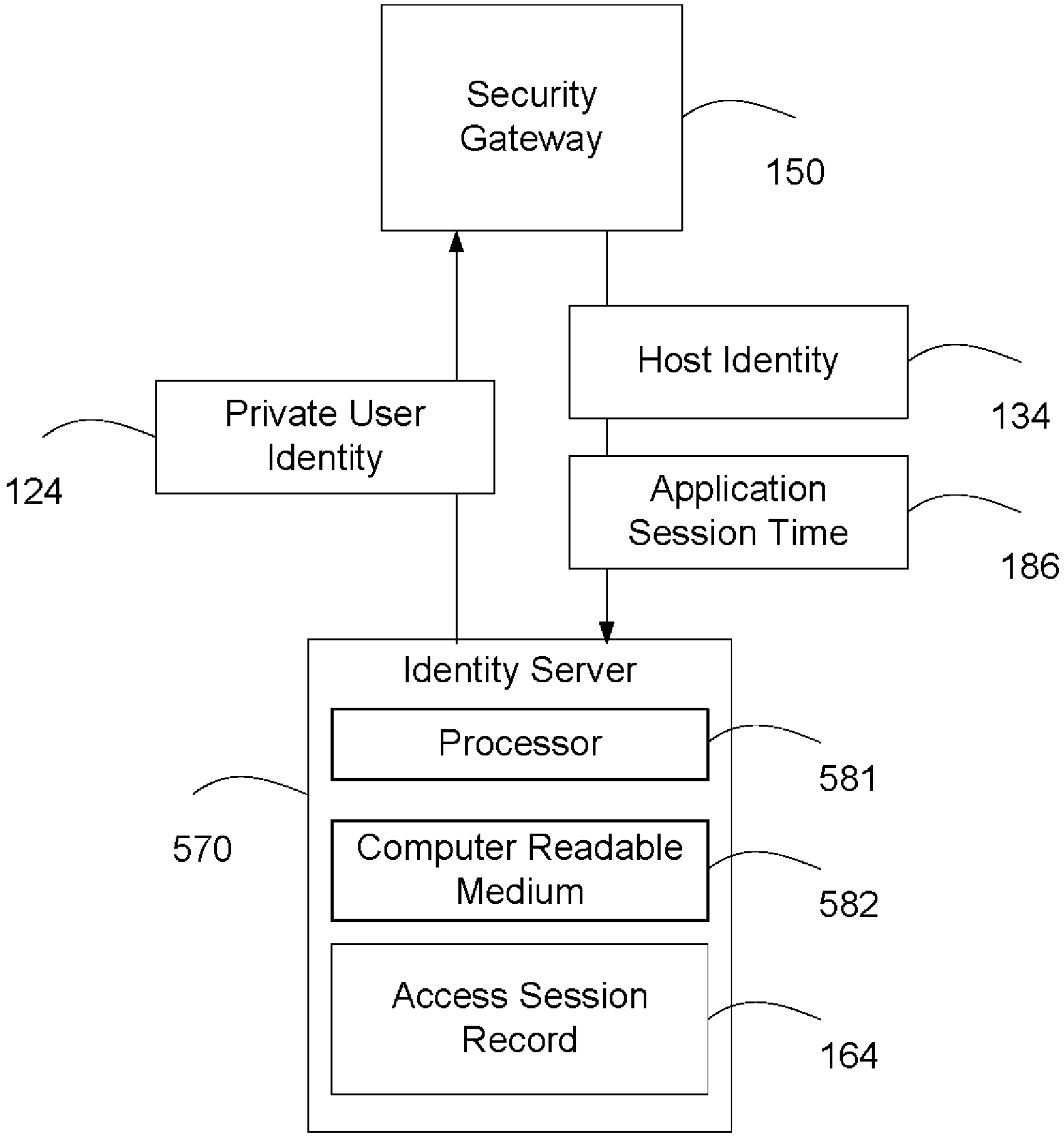

Security Gateway
150
Host Identity
134
Private User Identity
124
Application Session Time
186
Identity Server
Processor
581
570
Computer Readable Medium
582
Access Session Record
164

FIG. 5

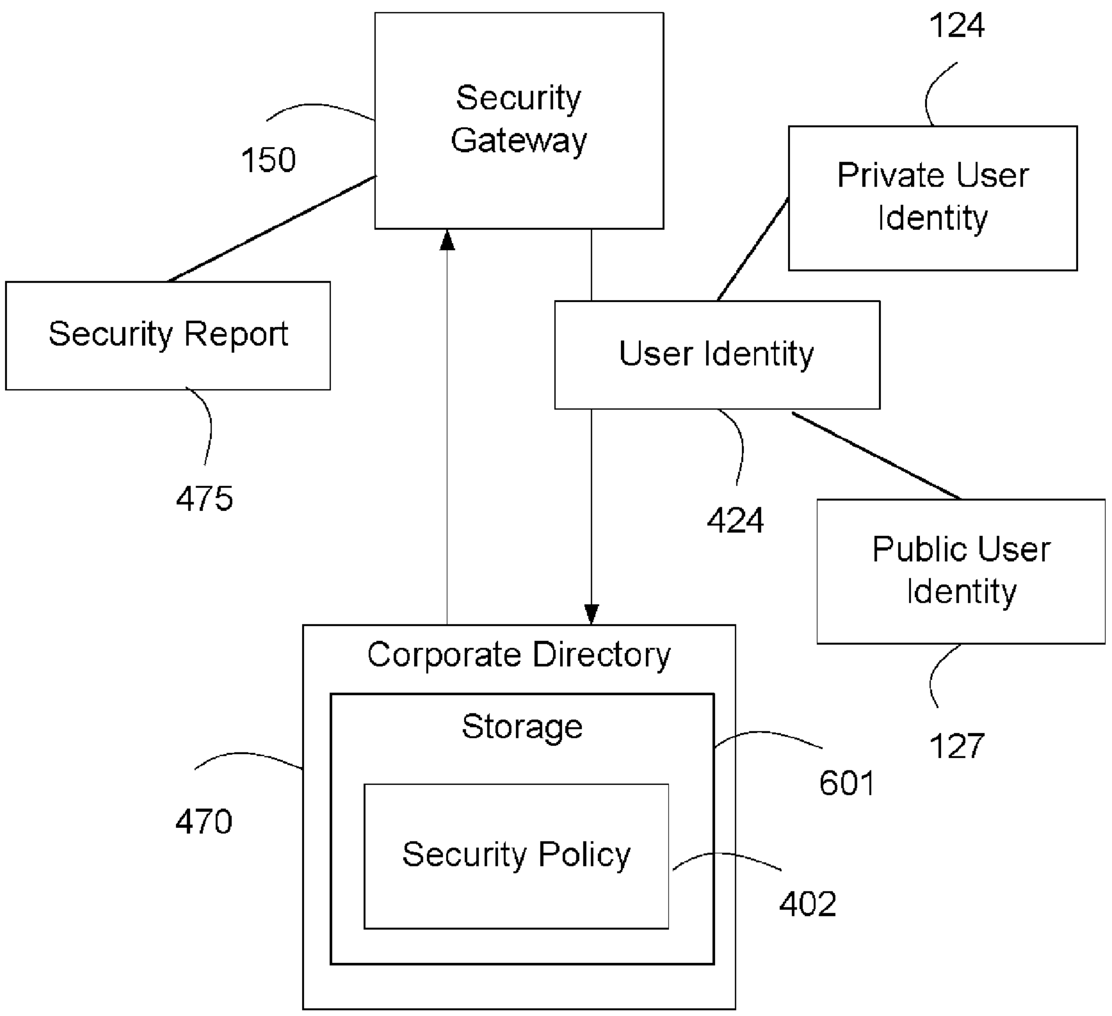

Security Gateway
150
124
Private User Identity
Security Report
User Identity
475
424
Public User Identity
Corporate Directory
Storage
127
601
470
Security Policy
402

FIG. 6

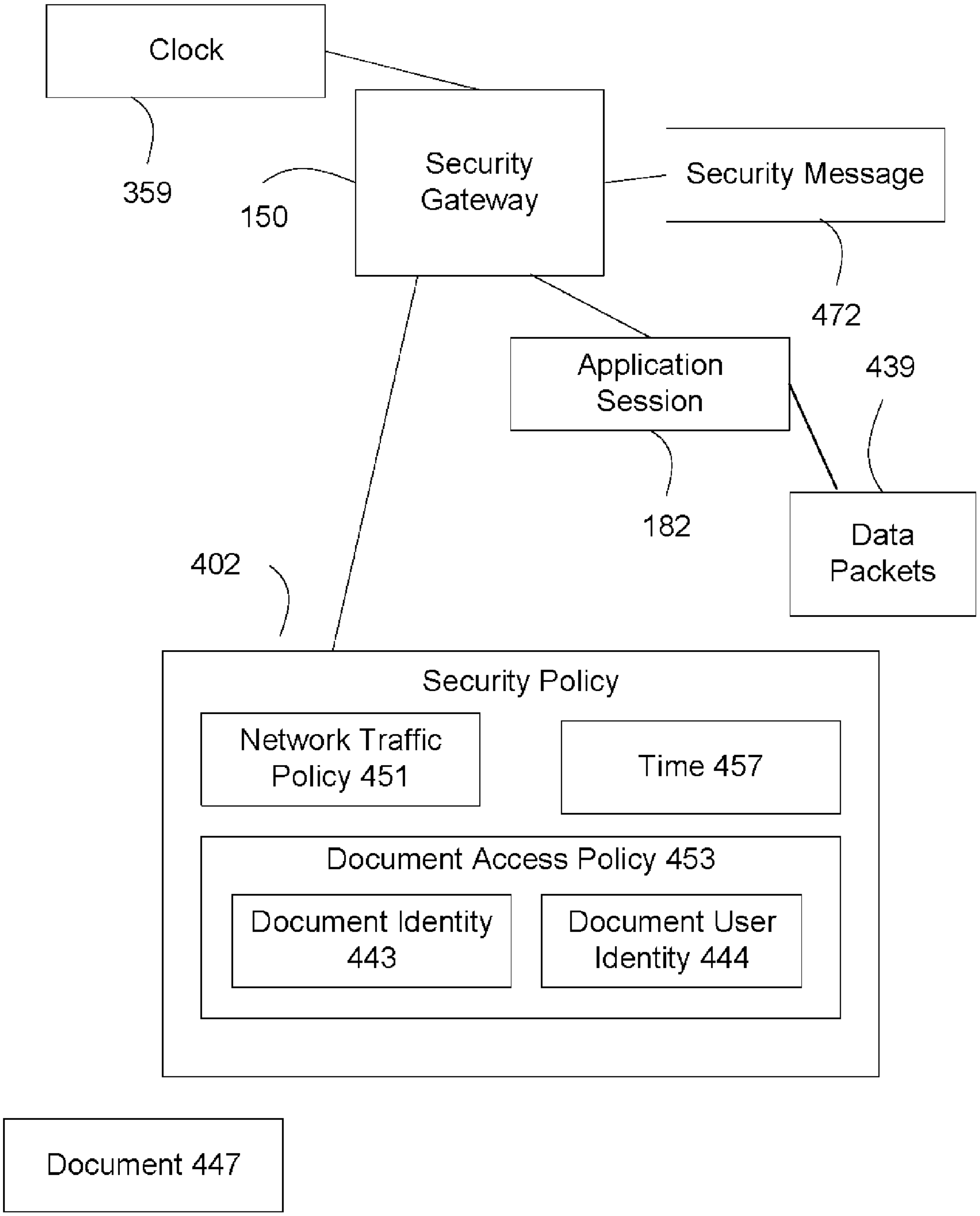

Clock
359
150
Security Gateway
Security Message
472
Application Session
439
182
Data Packets
402
Security Policy
Network Traffic Policy 451
Time 457
Document Access Policy 453
Document Identity 443
Document User Identity 444
Document 447

FIG. 7

Network Traffic Policy 451

Network based Application Session Access Control
Session Connection Rate Control
Traffic Shaping Control
Bandwidth Rate Capacity
Quality of Service or DSCP Marking Control
Packet Forwarding Control
Link Interface Preference
Server Load Balancing Preference
Application Session Modification Control

FIG. 8

APPLYING SECURITY POLICY TO AN APPLICATION SESSION

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application is a continuation and claims the priority benefit of U.S. patent application Ser. No. 14/061,720, filed on Oct. 23, 2013, issued on Aug. 19, 2014, as U.S. Pat. No. 8,813,180; which in turn is a continuation of U.S. patent application Ser. No. 13/650,179, filed on Oct. 12, 2012, issued on Nov. 26, 2013, as U.S. Pat. No. 8,595,791; which in turn is a continuation of U.S. patent application Ser. No. 12/788,339, filed on May 27, 2010, issued on Nov. 13, 2012 as U.S. Pat. No. 8,312,507; which in turn is a continuation-in-part of U.S. patent application Ser. No. 12/771,491, filed on Apr. 30, 2010, issued on Jul. 12, 2011, as U.S. Pat. No. 7,979,585; which in turn is a continuation of U.S. patent application Ser. No. 11/582,613, filed on Oct. 17, 2006, issued on May 11, 2010, as U.S. Pat. No. 7,716,378. The disclosures of each of the above referenced applications are hereby incorporated by reference.

BACKGROUND OF THE INVENTION

1. Field

This invention relates generally to data networking, and more specifically, to a system and method to apply a network traffic policy based on a user identity during an application session.

2. Related Art

The secure data network of a company is a critical component for day-to-day functioning of company business activities. Company employees access the secure data network for communication within the company and with the outside world. Company information, oftentimes proprietary or confidential, is exchanged during the communication.

Typically, an employee gains access to the company's secure data network by means of a network logon procedure using a private user identity, such as a user name "Robert P. Williamson" or an employee number "NG01-60410". Subsequent information exchange using the company's office applications, such as email, file transfer or document control is traceable based on the private user identity through network event logs.

Since the late 1990's, we have been witnessing the phenomenal rising popularity of public communication applications and services, such as email and Instant Messaging offered by Yahoo™, America Online™ (AOL), or Google™, conferencing and collaboration services offered by WebEx™ or Centra™, or peer-to-peer services for a variety of file sharing. Generally, a public communication service allows a user to exchange information through messaging, text chat or document exchange using a public user identity, such as "butterdragon", "fingemail1984", or "peterrabbit".

However, in a company setting, when an employee connects to a public communication service with a public user identity over the company's secure data network, the information exchange is not easily traceable if at all since the public user identity is not tied to the private user identity.

In one example, a company's information technology (IT) department notices that an employee Victor has been using the company's email system to send out proprietary documents, violating the company's security policy. After issuing a warning to Victor, the IT department finds no further violations. Unfortunately, they are not aware of the fact that Victor has continued this activity using Yahoo™ email with a public user identity "PiratesOfCaribbean@Yahoo.com".

In another example, two weeks before a major trade show, a company implements a security measure to monitor communication activities of employees of director level and above to ensure confidentiality of competitive information. This security measure, covering company email, phone conversation and voice messaging, nevertheless proves to be a failure as sensitive information leaks out to a business reporter anyway prior to the trade show. The source of the leak may never be confirmed, but the business reporter privately discloses that he gets the information from an anonymous employee of the company using AOL Instant Messaging™ with screen name "opensecret2006".

The above discussion illustrates the need for a security solution to associate a user identity to a public application.

BRIEF SUMMARY OF THE INVENTION

Method for applying a security policy to an application session, includes: recognizing the application session between a network and an application via a security gateway; determining by the security gateway a user identity of the application session using information about the application session; obtaining by the security gateway the security policy comprising network parameters mapped to the user identity; and applying the security policy to the application session by the security gateway. The user identity may be a network user identity or an application user identity recognized from packets of the application session. The security policy may comprise a network traffic policy mapped and/or a document access policy mapped to the user identity, where the network traffic policy is applied to the application session. The security gateway may further generate a security report concerning the application of the security policy to the application session.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1***a* illustrates a secure network.

FIG. **1***b* illustrates an access session and an application session.

FIG. **1***c* illustrates an access session record and an application session record.

FIG. **2** illustrates a process to generate an application session record.

FIG. **3** illustrates a process to recognize an application session.

FIG. **4***a* illustrates a process to determine a public user identity of application session.

FIG. **4***b* illustrates a data packet in an AIM log-on packet.

FIG. **5** illustrates a process to determine a private user identity.

FIG. **6** illustrates an embodiment of a security gateway obtaining a security policy by querying a corporate directory.

FIG. **7** illustrates a security policy including a security control.

FIG. **8** illustrates a plurality of embodiments of network traffic policy.

DETAILED DESCRIPTION OF THE INVENTION

FIG. **1***a* illustrates a secure network.

A secure network **160** includes a host **130**. User **120** uses host **130** to access a public application **180** hosted in application server **190**. Application server **190** is outside of secure network **160**. The network traffic between host **130** and application server **190** passes through security gateway **150**. The security gateway **150** is operationally coupled to a processor **171** and a computer readable medium **172**. The computer readable medium **172** stores computer readable program code for implementing the various embodiments of the present invention as described herein.

Host **130** is a computing device with network access capabilities. The host **130** is operationally coupled to a processor **173** and a computer readable medium **174**. The computer readable medium **174** stores computer readable program code for implementing the various embodiments of the present invention as described herein. In some embodiments, host **130** is a workstation, a desktop personal computer or a laptop personal computer. In some embodiments, host **130** is a Personal Data Assistant (PDA), a smartphone, or a cellular phone.

In some embodiments, secure network **160** is an Internet Protocol (IP) network. In some embodiments, secure network **160** is a corporate data network or a regional corporate data network. In some embodiments, secure network **160** is an Internet service provider network. In some embodiments, secure network **160** is a residential data network. In some embodiments, secure network **160** includes a wired network such as Ethernet. In some embodiments, secure network **160** includes a wireless network such as a WiFi network.

Public application **180** provides a service that allows user **120** to communicate with other users in a real-time fashion. In some embodiments, the service includes text chat. In some embodiments, the service includes a voice call or a video call. In some embodiments, the service includes a network game. In some embodiments, the service includes exchanging a document, such as sending or receiving a text document, a PowerPoint™ presentation, an Excel™ spreadsheet, an image file, a music file or a video clip. In some embodiments, the service includes a collaborative document processing such as creating a document, a business plan, an agreement, wherein user **120** collaborates with other users in a real time fashion. In some embodiments, the service includes a collaborative information exchange such as a conference call. In some embodiments, the service is a social networking service. In some embodiments, the service includes real-time collaboration and non real-time collaboration.

In one example, public application **180** provides America Online Instant Messenger™ service. In one example, public application **180** provides Yahoo Instant Messenger™ voice service. In some embodiments, public application **180** provides a file sharing service such as Kazaa™ file sharing service. In some embodiments, public application **180** provides a network game service such as Microsoft™ Network Game service. In some embodiments, public application **180** provides an on-line collaborative document processing such as Google Docs™, and Salesforce.com™. In some embodiments, public application **180** provides an on-line information exchange and communications such as WebEx™. In some embodiments, public application **180** provides live information streaming such as live video streaming, live audio streaming, and instantaneous picture uploading.

Security gateway **150** is situated at the edge of secure network **160**. Security gateway **150** connects secure network **160** to public application **180**. Security gateway **150** receives network traffic from secure network **160** and transmits the network traffic to application server **190**. Likewise, security gateway **150** receives network traffic from application server **190** and transmits the network traffic to secure network **160**.

In some embodiments, security gateway **150** includes the function of a corporate Wide Area Network (WAN) gateway. In some embodiments, security gateway **150** includes the function of a residential broadband gateway. In some embodiments, security gateway **150** includes the function of a WAN gateway for an Internet service provider.

FIG. **1***b* illustrates an access session and an application session.

User **120** uses host **130** to access secure network **160** during an access session **162**.

Host **130** has a host identity **134**. Host **130** uses host identity **134** to connect to secure network **160**. In some embodiments, host identity **134** includes an IP address. In some embodiments, host identity **134** includes a Media Access Control (MAC) address.

Within secure network **160**, user **120** has a private user identity **124**. In some embodiments, private user identity **124** is an employee number or an employee name. In some embodiments, private user identity **124** is an Internet service subscription identity. In some embodiments, access session **162** is established after a successful network user log-in procedure, such as an employee network log-in, for secure network **160** using private user identity **124**. Private user identity **124** is associated with host identity **134**. In some embodiments, host **130** is a guest computing device. Private user identity **124** is associated with an Ethernet switch port where host **130** connects. In this embodiment, private user identity **124** is a port number, an Ethernet interface identity, or an Ethernet VLAN identity.

User **120** uses host **130** to access public application **180** in an application session **182**. User **120** uses a public user identity **127** during application session **182**. In some embodiments, public application **180** prompts user **120** to log-in before establishing application session **182**. During the application user log-in procedure, user **120** provides to public application **180** public user identity **127**. In another embodiment, public application **180** selects a public user identity **127** for user **120** for application session **182**. In some embodiments, public user identity **127** is set up through a user registration process or a service subscription process. Network traffic in application session **182** passes through security gateway **150**.

FIG. **1***c* illustrates an access session record and an application session record.

Access session record **164** records information about access session **162**. The information includes private user identity **124**, host identity **134** and access session time **166**. In some embodiments, access session time **166** is the starting time when access session **162** is established. In some embodiments, access session time **166** includes the starting time and the ending time when user **120** finishes access session **162**. In some embodiments, access session time **166** is a time stamp for a time during access session **162**.

Application session record **184** records information about application session **182**. The information includes private user identity **124**, public user identity **127**, and application session time **186**. In some embodiments, the information further includes host identity **134**. In some embodiments, application session time **186** includes the starting time when application session **182** is established. In some embodiments, application session time **186** includes a time stamp during application session **182**. In some embodiments, application session time **186** includes a time stamp when security gateway **150** recognizes application session **182**.

FIG. **2** illustrates a process to generate an application session record.

The process of generating application session record **184** includes multiple steps.

In step **201**, security gateway **150** recognizes an application session.

In step **202**, security gateway **150** determines a public user identity of the application session.

In step **203**, security gateway **150** determines a private user identity using information about the application session.

FIGS. **3-5** illustrates steps **201-203** respectively.

FIG. **3** illustrates a process to recognize an application session.

Security gateway **150** inspects network traffic between host **130** and application server **190** to recognize application session **182** for public application **180**.

In some embodiments, security gateway **150** inspects data packet **339** between host **130** and application server **190** for the recognition of application session **182**.

Security gateway **150** includes an application identifier **355** for public application **180**. Application identifier **355** includes information for recognizing application session **182**. In some embodiments, application identifier **355** includes a transport layer information, such as Transmission Control Protocol (TCP) or User Diagram Protocol (UDP); and at least one transport port number, such as a TCP port number or a UDP port number. In some embodiments, application identifier **355** includes application layer information, such as one or more data filters wherein a data filter specifies a value and a position of the value in a data packet. In one example, a data filter is [byte 0 with value "0x52"]. In one example, a data filter is [byte 4-7 with ASCII value of "ADEH"].

Security gateway **150** matches data packet **339** against application identifier **355**.

In some embodiments, application identifier **355** includes transport protocol type of TCP and a destination TCP port number of 5190, the TCP port number used by AIM protocol. In this embodiment, data packet **339** is a TCP packet from host **130** to application server **190**. Security gateway **150** matches data packet **339** against application identifier **355** and determines that public application **180** provides AIM service.

Security gateway **150** creates application session record **184**. Security gateway **150** extracted the source IP address from the IP header of data packet **339**, and stores the source IP address as host identity **134**. In some embodiments, data packet **339** includes link layer information, such as a source MAC address; security gateway **150** extracts and stores the source MAC address as host identity **134**.

In some embodiments, security gateway **150** connects to a clock **359**. Clock **359** indicates the current time of day. Security gateway **150** stores the time of day indicated by clock **359** in application session time **186**.

FIG. **4***a* illustrates a process to determine a public user identity of application session **182**.

The method for determining public user identity **127** is typically specific to public application **180**. In some embodiments, data packet **339** is an application packet. For example, public application **180** provides AIM service; data packet **339** is an AIM packet.

An AIM packet includes multiple fields, for example

Command start field is a 1-byte data field starting at byte offset 0 having a fixed hexadecimal value "0x02";

Channel ID field is a 1-byte data field starting at byte offset 1;

Sequence number field is a 2-byte integer starting at byte offset 2;

Data field length field is a 2-byte data field starting at byte offset 4;

Family field is a 2-byte data field starting at byte offset 6; and

Subtype field is a 2-byte data field starting at byte offset 8.

An AIM log-on packet is a AIM packet with family field having a fixed hexadecimal value of "0x00 0x17" and subtype field having a fixed hexadecimal value of "0x00 0x06".

AIM log-on packet further includes buddy name length field, a 1-byte integer starting at byte offset 19, and a variable length buddy name field starting at byte offset 20. Buddy name length field indicates the length in bytes of buddy name field.

Security gateway **150** matches data packet **339** to determine if data packet **339** is an AIM log-on packet. In some embodiments, data packet **339** is an AIM log-on packet **400** illustrated in FIG. **4***b*. Security gateway **150** extracts buddy name length field **405**. Security gateway **150** furthers extracts buddy name field **407**. In this embodiment, buddy name length field **405** is integer "13" and buddy name field **407** is "JohnSmithI984". Security gateway **150** stores "JohnSmithI984" as public user identity **127** in application session record **184**.

In some embodiments, data packet **339** is not an AIM log-on packet. Security gateway **150** inspects another data packet from host **130**.

FIG. **5** illustrates a process to determine a private user identity.

Secure network **160** includes an identity server **570**. The identity server **570** is operationally coupled to a processor **581** and a computer readable medium **582**. The computer readable medium **582** stores computer readable program code for implementing the various embodiments of the present invention as described herein. Identity server **570** includes access session record **164** of access session **162** during which user **120** accesses application session **182**.

Security gateway **150** queries identity server **570**. Security gateway **150** sends host identity **134** and application session time **186** to identity server **570**.

Identity server **570** receives host identity **134** and application session time **186**. Identity server **570** matches host identity **134** and application session time **186** against access session record **164**. Identity server **570** determines that host identity **134** matches host identity of access session record **164**. Identity server **570** further determines that application session time **186** matches access session time **166** of access session record **164** as application session time **186** is between the starting time and the ending time of access session record **164**. Identity server **570** sends private user identity **124** of access session record **164** to security gateway **150** as a response to the query.

Security gateway **150** receives private user identity **124** from identity server **570**, and stores private user identity **124** in application session record **184**.

In some embodiments, security gateway **150** stores public user identity **127** in application session record **184** after recognizing a log-on approval indication for the public user identity **127** from public application **180**.

In some embodiments, security gateway **150** queries identity server **570** immediately after determining public user identity **127**. In some embodiments, security gateway **150** queries identity server **570** after application session **182** ends.

In some embodiments, security gateway **150** queries identity server **570** by sending a plurality of host identities in a bulk request; and receives a plurality of private user identities in a bulk response.

In some embodiments, application session record **184** includes additional user information associated with private user identity **124**, such as cubicle or office number, cubicle or office location, telephone number, email address, mail-drop location, department name/identity, or manager name.

In some embodiments, security gateway **150** obtains the additional user information from identity server **570**. In some embodiments, security gateway **150** obtains the additional user information by querying a different server, such as a corporate directory server, by using the private user identity **124** received from identity server **570**.

In some embodiments, public application **180** provides file transfer service using File Transfer Protocol (FTP) protocol or a proprietary protocol. In some embodiments, public application **180** provides email service using Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP) or Post Office Protocol version 3 (POP3) protocol.

By using the application session record, the private user identity **124** and the public user identity **127** for an application session **182** may be determined. In some embodiments as illustrated by FIG. **6**, upon determining the public user identity and the private user identity, security gateway **150** obtains security policy **402** for the application session **182** by querying corporate directory **470**. In an embodiment, corporate directory **470** comprises security policy **402**. In some embodiments, corporate directory **470** is a server computer comprising a storage **601** that includes security policy **402**. In some embodiments, corporate directory **470** is a database comprising security policy **402**. In another embodiment, corporate directory **470** is a software module with program code stored on a computer readable medium (not shown) running in a computer. In some embodiments, corporate directory **470** resides in identity server **570**. In some embodiments, corporate directory **470** uses directory technologies such as Microsoft Active Directory™, lightweight directory access protocol (LDAP) directory services, web services, directory services using Java™ technologies. In some embodiments, corporate directory **470** includes a policy server hosting security policy **402** and other policies.

Security gateway **150** queries corporate directory **470** for a security policy, where the query includes user identity **424**. User identity **424** may include private user identity **124** or public user identity **127**. Corporate directory **470** matches user identity **424** against security policy **402** and determines security policy **402** is applicable to user identity **424**. In some embodiments security policy **402** maps network parameters to a user identity and there is a match between user identity **424** and the user identity in the security policy **402**. In some embodiments, security policy **402** maps network parameters to a group identity (not shown) and user identity **424** is a member of the group identity. In response to finding the match between the user identity **424** and the user identity in the security policy **402**, corporate directory **470** sends security policy **402** to security gateway **150**.

In some embodiments, security gateway **150** generates security report **475** based on application session record **184** and security policy **402**. In some embodiments, security gateway **150** generates security report **475** based on a pre-determined user identity or a list of pre-determined user identities. For example, the security report may be generated based on an input of user identity or identities. In some embodiments, security gateway **150** generates security report **475** based on a pre-defined schedule or when requested by an operator.

In some embodiments, security policy **402** includes a security control function as illustrated in FIG. **7**. Security gateway **150** applies the security policy **402** received from corporate directory **470** in response to the query to application session **182**. Security policy **402** typically are configured by a company to protect against improper access to the company confidential documents and to protect against improper usage of the company secure network **160** vital for the company operation. In some embodiments, in response to receiving the security policy **402**, the security gateway **150** confirms that the received security policy **402** contains a user identity that matches the user identity **424** sent in the query. In response to the confirmation, the security gateway **150** applies the security policy **402** to the application session **182**. In FIG. **7**, security policy **402** includes network traffic policy **451** or document access policy **453**.

FIG. **8** illustrates a plurality of embodiments of network traffic policy **451**. In some embodiments, network traffic policy **451** specifies network based application session access control indicating if user identity **424** is denied or allowed to continue application session **182**. If denied, security gateway **150** may stop forwarding data packets **439** of application session **182**. In some embodiments, network traffic policy **451** specifies bandwidth rate capacity such as 1 Mbps, 100 MB per day, or 5 GB per month. In an embodiment, bandwidth rate capacity is measured in packets such as 100 packets per second, 10 thousand packets per day or 4 million packets per month. In some embodiments, network traffic policy **451** specifies a quality of service (QOS) mapped to user identity **424** for application session **182**. For example, network traffic policy **451** indicates a change of Differentiated Services Code Point (DSCP) marking in the data packets **439** of application session **182**. In some embodiments, network traffic policy **451** specifies a queuing delay, a queuing priority, a packet forwarding path, a link interface preference, a server load balancing preference, a packet routing policy, or other control to handle data packets **439** of application session **182**.

In some embodiments, network traffic policy **451** includes a traffic shaping control. In one example, traffic shaping control specifies a TCP profile such as a change of window segment size, or a TCP window adjustment.

In some embodiments, network traffic policy **451** indicates session connection rate control based on user identity **424** specifying a rate or capacity such as 10 session connections per second, 35 concurrent sessions, 100 sessions during lunch hour, 500 sessions a day, 24 voice sessions a day, or 75 file transfer sessions an hour. In some embodiments, network traffic policy **451** may specify, when exceeding the rate or capacity, if application session **182** is denied or data packets **439** of application session **182** are dropped.

In some embodiments, network traffic policy **451** includes application session modification control mapped to user identity **424**, specifying how data packets **439** of application session **182** are modified for the user with the user identity **424**. In one example, application session modification control specifies security gateway **150** should perform network address translation (NAT) to application session **182** for user identity **424**. In one example, security gateway **150** should perform port address translation (PAT) to application session **182** using a pre-determined port number for user identity **424**. In another example, security gateway **150** should perform content substitution if application session **182** is a HTTP session and if a Universal Resource Locator (URL) in data packets **439** of application session **182** matches a pre-determined URL for user identity **424**. In an example, security gateway **150** should perform filename substitution if application session **182** is a file transfer session and if a filename matching a pre-determined filename is found in data packets **439** of application session **182** for user identity **424**. In another example, security gateway **150** should insert a cookie for user identity **424** if application session **182** is an HTTP session, with optionally data packets **439** matching a pre-determined POST or GET request of a URL.

Returning to FIG. **7**, in some embodiments, document access policy **453** specifies if access to document **447** is allowed or denied. In some embodiments, document **447** includes a file, a business agreement, a contract, a spreadsheet, a presentation, a drawing, a textual document, a manual, a program, a piece of software program, a design, a product specification, a datasheet, a video file, an audio file, an email, a voice mail, a fax, a photocopy of a document, or any business document. In some embodiments, document **447** includes an URL leading to digital information such as database query result, a web page, a video, or a piece of music. In some embodiments, document **447** includes real time transfer or streaming of information such as video streaming, audio streaming, a web cast, a podcast, a video show, a teleconference session, or a phone call. In some embodiments, document access policy **453** includes document identity **443** and document user identity **444**. Document identity **443** identifies document **447**. Document user identity **444** identifies the user whose access to the document **447** is affected by the document access policy **453**. In an embodiment, security gateway **150** compares user identity **424** with document user identity **444**. In response to determining that the user identity **424** matches the document user identity **444**, in some embodiments, security gateway **150** allows document **447** with document identity **443** to be accessed by user identity **424**. In another embodiment, security gateway **150** denies access to document **447** with document identity **443**. In denying access, the security gateway **150** may disconnect application session **182** or discard data packets **439**. In some embodiments, security gateway **150** confirms that data packets **439** include document identity **443**. In response to confirming that data packets **439** include document identity **443**, security gateway **150** applies document access policy **453**.

In some embodiments security policy **402** includes time **457** where security policy **402** is applicable within time **457**. In some embodiments, time **457** indicates a beginning time such as 8 am, 4 pm, midnight. In an embodiment, time **457** indicates a time range such as 8 am to 10 am, 7 pm to 5 am, morning hours, lunch, rush hour, prime time. Security gateway **150** compares clock **359** with time **457** and determines if security policy **402** is applicable.

In some embodiments, security gateway **150** generates security message **472** when security gateway **150** determines if security policy **402** is applicable to application session **182** for user identity **424**. In some embodiments, security gateway generates security message **472** when security gateway **150** applies security policy **402** to application session **182**. In some embodiments, security report **475** includes security message **472**. In one example, security message **472** includes security policy **402** and user identity **424**. In one example, security message **472** includes the actions security gateway **150** applies to application session **182** using security policy **402**.

The invention can take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment containing both hardware and software elements. In a preferred embodiment, the invention is implemented in software, which includes but is not limited to firmware, resident software, microcode, etc.

Furthermore, the invention can take the form of a computer program product accessible from a computer-usable or computer-readable medium providing program code for use by or in connection with a computer or any instruction execution system. For the purposes of this description, a computer-usable or computer readable medium can be any apparatus that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device.

The medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or a propagation medium. Examples of a computer-readable medium include a semiconductor or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disk and an optical disk. Current examples of optical disks include compact disk—read only memory (CD-ROM), compact disk—read/write (CD-R/W) and DVD.

A data processing system suitable for storing and/or executing program code will include at least one processor coupled directly or indirectly to memory elements through a system bus. The memory elements can include local memory employed during actual execution of the program code, bulk storage, and cache memories which provide temporary storage of at least some program code in order to reduce the number of times code must be retrieved from bulk storage during execution.

Input/output or I/O devices (including but not limited to keyboards, displays, point devices, etc.) can be coupled to the system either directly or through intervening I/O controllers.

Network adapters may also be coupled to the system to enable the data processing system to become coupled to other data processing systems or remote printers or storage devices through intervening private or public networks. Modems, cable modem and Ethernet cards are just a few of the currently available types of network adapters.

Foregoing described embodiments of the invention are provided as illustrations and descriptions. They are not intended to limit the invention to precise form described. In particular, it is contemplated that functional implementation of invention described herein may be implemented equivalently in hardware, software, firmware, and/or other available functional components or building blocks, and that networks may be wired, wireless, or a combination of wired and wireless. Other variations and embodiments are possible in light of above teachings, and it is thus intended that the scope of invention not be limited by this Detailed Description, but rather by the Claims following.

What is claimed is:

1. A method for applying a security policy to an application session, comprising:

recognizing the application session between a network and an application via a security gateway;

retrieving, by the security gateway, an application session record for the application session, the application session record comprising a first user identity used for accessing the application through a first host, a first host identity for the first host, and an application session time;

recognizing, by the security gateway, an access session between a second host and the network;

retrieving, by the security gateway, an access session record for the access session, the access session record comprising a second user identity used for accessing the network through the second host, a second host identity for the second host, and an access session time;

querying, by the security gateway, an identity server by sending the first host identity and the application session time in the application session record, the identity server comprising the access session record for the access session between the second host and the network;

comparing, by the identity server, the first host identity in the application session record with the second host identity in the access session record, and comparing the access session time with the application session time;

returning, by the identity server, the second user identity in the access session record if the first host identity in the application session record matches the second host identity in the access session record, and if the access session time matches the application session time;

storing, at the identity server, the second user identity as a network user identity used for accessing the network in the application session record;

determining, by the security gateway, at least one security policy applicable to the application session based on a group identity; and

applying the at least one security policy to the application session by the security gateway if the network user identity is a member of the group identity.

2. The method of claim **1**, wherein the determining, by the security gateway, at least one security policy applicable to the application session further comprises determining that the at least one security policy is applicable for the time period.

3. The method of claim **1**, wherein the at least one security policy comprises a network traffic policy.

4. The method of claim **3**, wherein the network traffic policy comprises a bandwidth rate capacity for the network.

5. The method of claim **3**, wherein the network traffic policy comprises a quality of service mapped to the network user identity for the application session.

6. The method of claim **3**, wherein the network traffic policy comprises one or more of: a queuing delay, a queuing priority, a packet forwarding path, a link interface preference, a server load balancing preference, and a packet routing policy.

7. The method of claim **3**, wherein the network traffic policy comprises a traffic shaping control.

8. The method of claim **7**, wherein the traffic shaping control comprises a TCP profile.

9. The method of claim **3**, wherein the network traffic policy comprises an application session modification control based on the network user identity.

10. A computer program product for applying a security policy to an application session, the computer program product comprising:

a non-transitory computer readable storage medium having computer readable program code embodied thereon, the computer readable program code configured to:

recognize the application session between a network and an application via a security gateway;

retrieve, by the security gateway, an application session record for the application session, the application session record comprising a first user identity used for accessing the application through a first host, a first host identity for the first host, and an application session time;

recognize, by the security gateway, an access session between a second host and the network;

retrieve, by the security gateway, an access session record for the access session, the access session record comprising a second user identity used for accessing the network through the second host, a second host identity for the second host, and an access session time;

query, by the security gateway, an identity server, by sending the first host identity and the application session time in the application session record, the identity server comprising the access session record for the access session between the second host and the network;

compare, by the identity server, the first host identity in the application session record with the second host identity in the access session record, and compare the access session time with the application session time;

return, by the identity server, the second user identity in the access session record if the first host identity in the application session record matches the second host identity in the access session record, and if the access session time matches the application session time;

store, at the identity server, the second user identity as a network user identity used for accessing the network in the application session record;

determine, by the security gateway, at least one security policy applicable to the application session based on a group identity; and

apply the at least one security policy to the application session by the security gateway, if the network user identity is a member of the group identity.

11. The computer program product of claim **10**, wherein the computer readable program code configured to determine, by the security gateway, at least one security policy applicable to the application session is further configured to determine that the at least one security policy is applicable for the time period.

12. The computer program product of claim **10**, wherein the at least one security policy comprises a network traffic policy.

13. The computer program product of claim **12**, wherein the network traffic policy comprises a bandwidth rate capacity for the network.

14. The computer program product of claim **12**, wherein the network traffic policy comprises a quality of service mapped to the network user identity for the application session.

15. The computer program product of claim **12**, wherein the network traffic policy comprises one or more of: a queuing delay, a queuing priority, a packet forwarding path, a link interface preference, a server load balancing preference, and a packet routing policy.

16. The computer program product of claim **12**, wherein the network traffic policy comprises a traffic shaping control.

17. The computer program product of claim **16**, wherein the traffic shaping control comprises a TCP profile.

18. The computer program product of claim **12**, wherein the network traffic policy comprises an application session modification control based on the network user identity.

19. A system, comprising:

a corporate directory comprising at least one security policy; and

a security gateway, wherein the security gateway:

recognizes an application session between a network and an application;

retrieves an application session record for the application session, the application session record comprising a first user identity used for accessing the application through a first host, a first host identity for the first host, and an application session time;

recognizes an access session between a second host and the network;

retrieves an access session record for the access session, the access session record comprising a second user identity used for accessing the network through the second host, a second host identity for the second host, and an access session time;

queries an identity server by sending the first host identity and the application session time in the application session record, the identity server comprising the access session record for the access session between the second host and the network, wherein the identity server:

compares the first host identity in the application session record with the second host identity in the access session record, and compares the access session time with the application session time;

returns the second user identity in the access session record if the first host identity in the application session record matches the second host identity in the access session record, and if the access session time matches the application session time; and

stores the second user identity as a network user identity used for accessing the network in the application session record;

determines at least one security policy applicable to the application session based on a group identity; and

applies the at least one security policy to the application session if the network user identity is a member of the group identity.

20. The system of claim **19**, wherein the determines at least one security policy applicable to the application session further comprises determines that the at least one security policy is applicable for the time period.

21. The system of claim **19**, wherein the at least one security policy comprises a network traffic policy.

22. The system of claim **21**, wherein the network traffic policy comprises a bandwidth rate capacity for the network.

23. The system of claim **21**, wherein the network traffic policy comprises a quality of service mapped to the network user identity for the application session.

24. The system of claim **21**, wherein the network traffic policy comprises one or more of: a queuing delay, a queuing priority, a packet forwarding path, a link interface preference, a server load balancing preference, and a packet routing policy.

25. The system of claim **21**, wherein the network traffic policy comprises a traffic shaping control.

26. The system of claim **25**, wherein the traffic shaping control comprises a TCP profile.

27. The system of claim **21**, wherein the network traffic policy comprises an application session modification control based on the network user identity.

* * * * *